ENCLOSURE 2

THE DEFENSE INFORMATION INFRASTRUCTURE (DII)

1.0 Why the DII?

The National Military Strategy dictates that Department of Defense (DoD) have agile, sustained, worldwide access to information and communications as it trains for and responds to crises and regional conflicts. The DoD information systems that make up the existing DII do not fully support these requirements. DoD-wide assessments following Desert Storm have recognized four operational realities:

- Availability of information is key to warfighting.
- Support for migration applications evolution is key to containing functional costs.
- Legacy operations costs severely impact modernization.
- Stovepipe approaches to information technology modernization limit interoperability, effectiveness and joint warfighting.

2.0 Definition of the DII.

The DII is a seamless web of communications networks, computers, software, databases, applications, data and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles. It includes:

- The physical facilities used to collect, distribute, store, process, and display voice, data and imagery;
- The applications and data engineering practices (tools, methods, and processes) to build and maintain the software that allow C^2, Intelligence, and Mission Support users to access and manipulate, organize and digest proliferating quantities of information;
- The standards and protocols that facilitate interconnection and interoperation among networks and systems and that provide security for the information carried; and
- The people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities and train others in DII capabilities and use.

3.0 Scope of the DII.

The DII provides information products and services for the DoD Services and Agencies. The current DII is made up of many elements, as shown in Figure E.2-1. Each element of the DII is connected, much like the pieces of a puzzle. And, like a puzzle, the DII is not complete without every piece intact. No single piece is meaningful when it is separated from the rest, but a single missing piece will impact the whole picture.

3.1 Foundation. DII elements build on and include a foundation of integration and technology support elements. The base includes modeling and simulation capabilities to assess the need for changed services, continual assessment of new technology as it could be applied to the DII, transport and processing standards, thorough testing, appropriate levels of information security, modern software engineering practices and sound architecture policy.

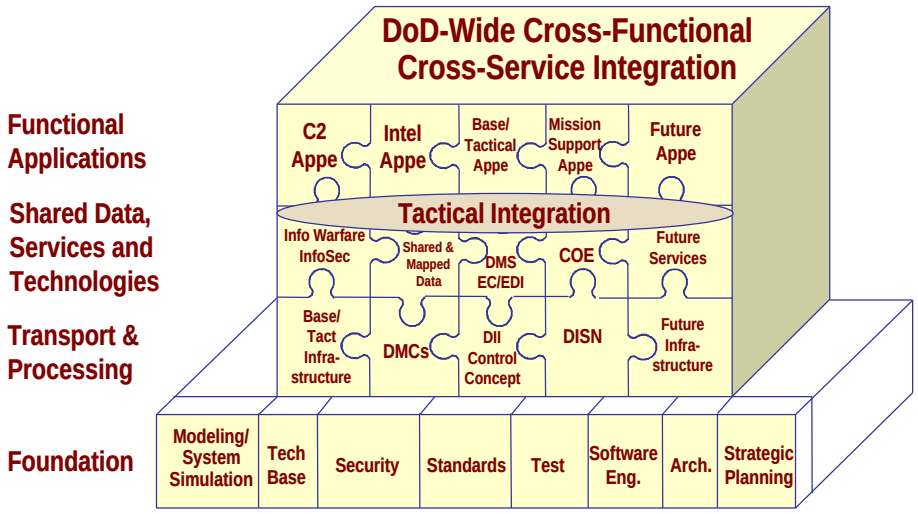


Figure E.2-1. Elements of the DII

3.2 Technical Infrastructure. The Technical Infrastructure of the DII includes the Defense Information System Network (DISN) communications base; the Defense Megacenters for handling major information system processing and maintenance; and the DII Control Concept to manage the DII network and systems. These enterprise level elements of the DII interface with the Base/Tactical (Local) Infrastructure (e.g., Sustaining Base Information Services (SBIS)) to provide the end-to-end DoD Technical Infrastructure for data collection, distribution, processing, storage and display. The DII Control Concept provides Global, Regional and Local control centers to manage the technical infrastructure of the DII.

The elements of the DII include applications in all DoD mission areas; shared data, services and technologies; the technical infrastructure; and a foundation of technology support.

Technical Integration provides the glue for the DII elements.

3.3 Shared Services. Shared Services provide cross-functional, cross-organization capabilities for interpersonal and interorganizational messaging through Defense Message System (DMS) and support electronic commerce (e.g. procuring, provisioning, shipping, making payments) through Electronic Data Interchange (EC/EDI). The DII Common Operating Environment (COE) provides a set of integrated common support services and a corresponding software development environment for functional applications. The DII COE provides common services and enables execution and integration of joint and service mission applications. Shared Data supports interoperability of Functional Applications at the data level among Services and functional areas as needed to conduct the DoD's mission.

3.4 Functional Applications. Functional Applications include all DoD mission areas: Command and Control (C^2) (e.g., Global Command and Control System (GCCS)), including tactical applications; Intelligence (e.g., the DoD Intelligence Information System (DoDIIS), Tactical Initiatives and Related Activities (TIARA) and INTELINK); and Mission Support (e.g., Global Combat Support System (GCSS)). Functional Applications depend upon shared services, data, and technologies to provide the environment for sharing information among functional communities. Functional applications also rely upon the information processing and transport capabilities of the DII Technical Infra-

structure to deliver service to their functional communities. Finally, technical integration and cross-service/cross-functional integration provide the glue holding the DII elements together.

4.0 DII Baseline Characterization.

The present DII is largely an unintegrated collection of systems. As such, it only partially meets the requirements of the DoD mission support and warfighting communities. Because it is unintegrated, there are redundancies and duplications that increase the cost of operations and thereby reduce the total resources focused on the DoD warfighting mission.

- The infrastructure is fragmented by multiple "stovepipe" systems. This inhibits interoperability necessary to give Commanders a unified picture of the battlespace; to provide links between the battlefield and the power projection support base; and to connect DoD to the U.S. Industrial Base.
- There is unnecessary redundancy and duplication of infrastructure elements. This results in waste and excessive cost that takes dollars and manpower away from vital warfighting capabilities.
- The infrastructure is not planned, architected/engineered, acquired and operated from a Defense-wide perspective. This lack of Defense-wide perspective means that each mission may develop its own capabilities instead of sharing common solutions, and the solutions may not be interoperable and integrated.

There are three major areas of DII interdependencies: functional applications, local infrastructure and enterprise infrastructure.

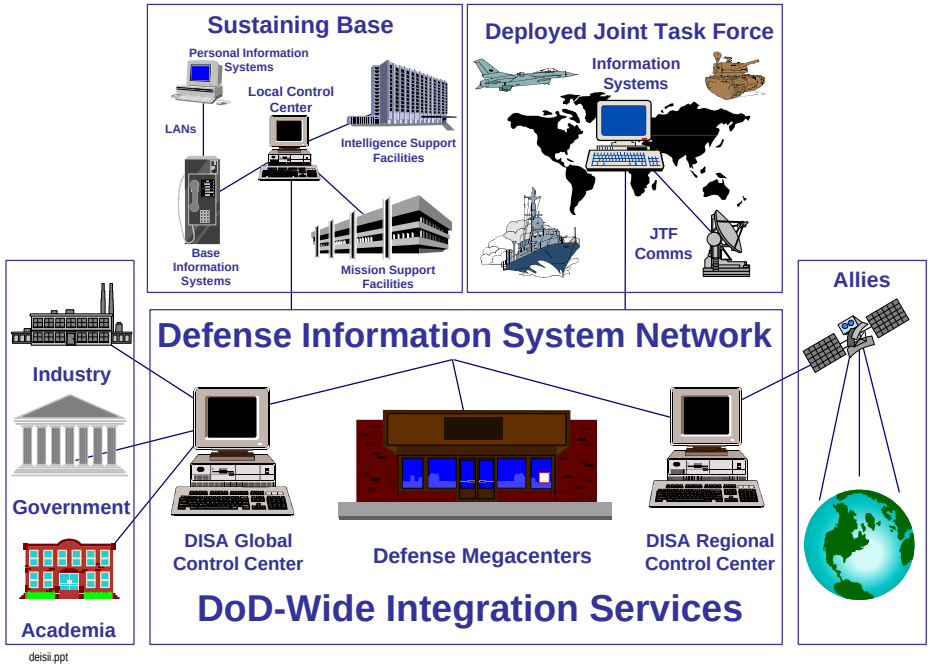
Furthermore, existing capabilities are not adequate to meet current changes in mission, policy, and doctrine that are part of new warfighting and fiscal realities. For the Warfighter, these realities include the need to support combined and joint peacetime operations worldwide, to fight two simultaneous major regional conflicts anywhere, to adapt to flexible and changing force compositions, and to deploy a significant force rapidly and support that force from the CONUS and in-theater sustaining base.

5.0 DII Goal Architecture.

Figure E.2-2 shows the DII, its components and their relationships for the objective environment. The DII includes the enterprise information infrastructure, the deployed Combined/Joint Task Force (C/JTF) information infrastructure, and the Sustaining Base/Afloat information infrastructure. The figure illustrates the cross-functional and cross-organizational nature of the DII architecture. It is the sum of all parts that constitute the information management assets owned by each of the components, including OSD, the Joint Staff, the individual Services, Agencies and others. As such, the DII requires cooperative development reflective of its cooperative ownership.

The DII serves the deployed C/JTF, the Sustaining Base and Enterprise Services.

To support the goals of C^4IFTW, DII users must be able to work collaboratively, access information and resources when needed and from any location and reach other users on interconnected networks via voice, data, video, or some combination, while maintaining the security required to preserve the integrity of military operations. DII users must be able to work with data and applications across functions.



E.2-2 - The DII Goal Architecture

The DII will operate as a collection of distributed heterogeneous information systems. It must continue to support legacy systems while evolving to support new and existing missions. Information will be stored in many ways and at many levels of detail. Applications within the DII will range from centrally developed DoD applications implemented at central locations to base-level or end-user applications residing on the desktop or in tactical environments. Computing and communications environments will range from supercomputers to client/ server processing to desktop computers and will extend into the battlefield. By the year 2000, many of the systems will be standards-based, but will continue to contain legacy elements that are proprietary in nature. The DII will evolve in the future by integrating these components as well as introducing new technology.

6.0 DII Interdependencies.

Figure E.2-3 shows three major components of the DII which are interdependent: functional applications, base/tactical infrastructure and enterprise infrastructure. These three components approximate the division of responsibilities shared respectively by the PSAs and the Joint Chiefs of Staff (JCS) (functional applications), CINCs/Services/ Agencies (local infrastructure) and Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C^3I)) and DISA (enterprise infrastructure). As shown in the figure, parts of these three domains are interdependent.

The three interdependent components provide for the DII goal of supporting national policy that calls for the ability to plug in and access information anywhere and anytime. This is made possible by the elements of the enterprise infrastructure that allow the other two components to develop systems that are interoperable and secure from the base to the Warfighter. For example, the Technical Architecture Framework for Information Management (TAFIM) standards and services, as expanded on by the DII Architecture, the DII Common Operating Environment (COE), the DoD Data Administration Strategic Plan, and the DoD Goal Security Architecture (DGSA) Transition Plan, provide a common basis for implementing mission area applications such as the GCCS for the C^2 community. The

base/tactical (local) infrastructure builds solutions on common standards and services that are provided by the enterprise infrastructure. The enterprise infrastructure must, in turn, provide standards and services that facilitate meeting the goals of national policy and C4IFTW. In addition, the enterprise infrastructure provides the interface between DoD and the rest of the Federal Government. Facilitating cost-effective and responsive functional applications at the Enterprise and Local (Base, Deployed/Afloat) levels requires continuing coordination among the CINCs/Service/Agencies, PSAs, JCS, ASD(C3I) and DISA.

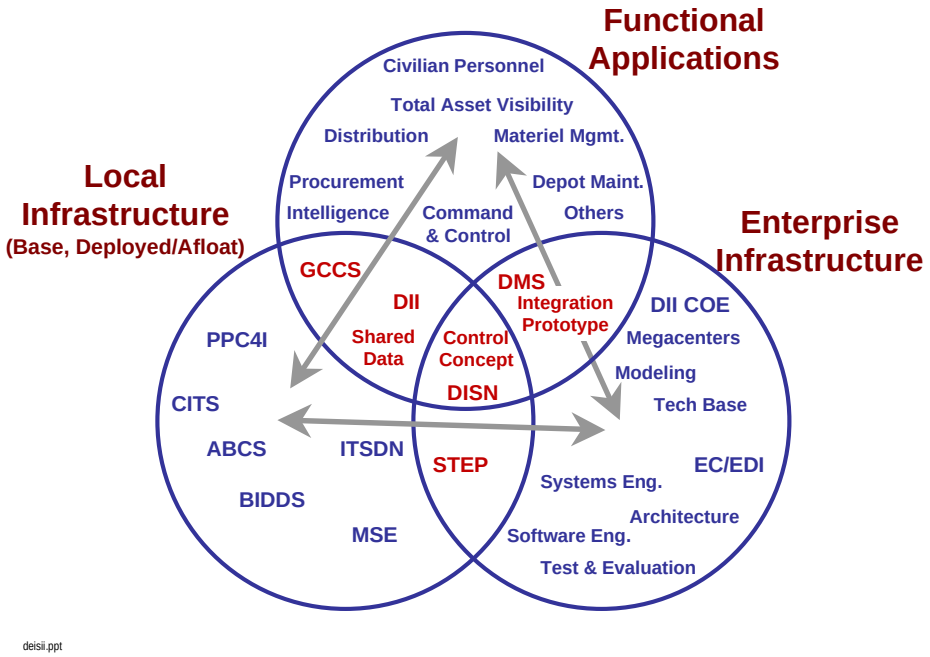


Figure E.2-3 - DII Interdependencies

7.0 Relationship of the DII and National Information Infrastructure (NII).

The NII is a Federal-level enterprise, in concert with industry and state and local Governments, to develop a national high-speed information processing and transfer network. Evolution of the NII includes national telecommunications policy reform to encourage growth of the information industry. The NII is by definition national in scope. The scope of the DII is international. The DII uses the NII in combination with U.S./Allied Military and commercial oversees information infrastructure to meet the global information needs of the DoD.

> ***The DII uses the NII in combination with U.S./Allied Military and commercial oversees information infrastructure to meet the global information needs of the DoD.***

The DII provides interfaces for DoD customers to other sources in the NII and to U.S. Allies. The DII also can provide information services to selected non-DoD customers. For example, service could be extended globally for NII customers through existing DII capabilities. Also, strategic cooperation between the DII and the NII organizations will foster development of dual-use technologies, technology transfer, information technology standards and defense conversion to reduce the cost to the Government of providing information services while increasing U.S. global competitiveness in information technologies.